

Théorie de la Divisibilité

1) Définition axiomatique des diviseurs

$\mathcal{D}$ = anneau intègre et unitaire

Def : Une Théorie des diviseurs sur $\mathcal{D}$ est la donnée d'un monoïde commutatif unitaire Δ sur lequel la décomposition en facteurs premiers existe et est unique, et d'un homomorphisme multiplicatif

$$\begin{aligned}\mathcal{D}^* &\longrightarrow \Delta \\ \alpha &\longmapsto (\alpha)\end{aligned}$$

tg

1) Si $\alpha, \beta \in \mathcal{D}^*$ $\alpha | \beta$ dans $\mathcal{D} \iff (\alpha) | (\beta)$ dans Δ

2) Si $\alpha, \beta \in \mathcal{D}$ et $\alpha \in \Delta$, alors $\alpha | \alpha$ et $\alpha | \beta \Rightarrow \alpha | \alpha \pm \beta$
(condition que $\alpha | \alpha$ ssi $\alpha | (\alpha)$)

3) Si $\alpha, \beta \in \Delta$,

$$\alpha = \beta \iff \{ \alpha \in \mathcal{D} / \alpha | \alpha \} = \{ \alpha \in \mathcal{D} / \beta | \alpha \}$$

ie $\alpha = \beta$ ssi les multiples de α dans $\mathcal{D}$ coïncident avec ceux de β , dans $\mathcal{D}$.

Def:

Les éléments de Δ sont les diviseurs de $\mathcal{D}$

Si $\alpha \in \mathcal{D}^*$, (α) s'appelle un diviseur principal.

La condition 1) de la Def. entraîne :

Pr

$$(\alpha) = (\beta) \iff \alpha \text{ et } \beta \text{ sont associés dans } \mathcal{D}$$

$$(\alpha) = e \text{ élément unité de } \Delta \iff \alpha \text{ unité.}$$

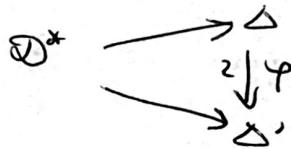
ex : $\mathcal{D} = \mathbb{Z}$, $\Delta = \mathbb{N}$

$\mathcal{D}^* \longrightarrow \mathbb{N}$ définit une Théorie des diviseurs
 $\alpha \longmapsto |\alpha|$ sur $\mathbb{Z}$.

2) Unicité d'une Théorie des diviseurs.

Th. Une Théorie des diviseurs sur $\mathcal{D}$ est unique à isomorphisme près.

Si $\mathcal{D}^* \rightarrow \Delta$ et $\mathcal{D}^* \rightarrow \Delta'$ sont 2 Théories des diviseurs sur $\mathcal{D}$, alors il existe un isomorphisme $\varphi: \Delta \rightarrow \Delta'$ qui fait se correspondre les diviseurs principaux.



preuve: Soient

$\mathfrak{p} \in \Delta$ diviseur premier $\bar{\mathfrak{p}} = \text{multiples de } \mathfrak{p} \text{ dans } \mathcal{D}$

$\mathfrak{p}' \in \Delta'$ " " $\bar{\mathfrak{p}}' = \text{" de } \mathfrak{p}' \text{ dans } \mathcal{D}$

* Alors $\forall \mathfrak{p} \in \Delta \exists \mathfrak{p}' \in \Delta' \bar{\mathfrak{p}}' \subset \bar{\mathfrak{p}}$ (1)

Par l'absurde. Sinon, on aurait $\bar{\mathfrak{p}}' \not\subset \bar{\mathfrak{p}}$ pour tout diviseur premier $\mathfrak{p}' \in \Delta'$.

Soit $\beta \neq 0$ un él. de $\mathcal{D}$ divisible par $\mathfrak{p}$. Par déc. en facteurs premiers dans Δ' :

$$(\beta) = \mathfrak{p}_1^{R_1} \dots \mathfrak{p}_n^{R_n}$$

et $\bar{\mathfrak{p}}'_i \not\subset \bar{\mathfrak{p}} \quad \forall i \Rightarrow \exists \gamma_i \in \mathcal{D} \quad \gamma_i \text{ divisible par } \mathfrak{p}'_i \text{ et non par } \mathfrak{p}$

$\gamma \doteq \gamma_1^{R_1} \dots \gamma_n^{R_n}$ sera divisible par $(\beta) = \mathfrak{p}_1^{R_1} \dots \mathfrak{p}_n^{R_n}$, donc par β , donc par $\mathfrak{p}$.

C'est absurde car :

$$\left\{ \begin{array}{l} \mathfrak{p} \text{ premier} \\ \mathfrak{p} \mid (\gamma) = (\gamma_1)^{R_1} \dots (\gamma_n)^{R_n} \\ \mathfrak{p} \text{ ne divise aucun } \gamma_i \end{array} \right.$$

d'où (1).

* De la même manière :

$$\exists q \in \Delta \quad \bar{q} \subset \bar{p}'$$

desorte que :

$$\forall p \in \Delta \quad \exists p', q \quad \bar{q} \subset \bar{p}' \subset \bar{p} \quad (2)$$

* Montrons que $q = p'$ (3)

Il existe $\xi \in \Delta$ / $q \mid \xi$ et $q \cdot p' \nmid \xi$ (condition 3))

Si $q \neq p'$, ξ ne serait pas divisible par p' , ce qui contredit $\bar{q} \subset \bar{p}'$.

* Conclusion :

$$\left. \begin{array}{l} (2) \\ (3) \end{array} \right\} \Rightarrow \bar{p} = \bar{p}'$$

De plus, ^{si p' est donné} il existe 1 et 1 seul diviseur p de Δ tel que $\bar{p} = \bar{p}'$ (condition 3), et l'on peut définir la bijection :

$$\begin{array}{ccc} \varphi : \text{diviseurs premiers de } \Delta & \longrightarrow & \text{diviseurs premiers de } \Delta' \\ p & \longmapsto & p' / \bar{p}' = \bar{p} \end{array}$$

que l'on prolonge de façon unique de $\Delta \rightarrow \Delta'$ en posant :

$$\begin{array}{ccc} \varphi : \Delta & \longrightarrow & \Delta' \\ p_1^{k_1} \dots p_r^{k_r} & \longmapsto & p_1'^{k_1} \dots p_r'^{k_r} \quad (\text{où } \bar{p}_i' = \bar{p}_i) \end{array}$$

* φ fait correspondre les diviseurs principaux :

$$\text{NB: } (\alpha) \in \Delta \quad (\alpha) = \mathfrak{p}^k \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_s^{e_s}$$

$$(\alpha)' \in \Delta' \quad (\alpha)' = \mathfrak{p}'^m \mathfrak{p}'_1^{e'_1} \dots \mathfrak{p}'_s^{e'_s}$$

$$\text{où } \varphi(\mathfrak{p}) = \mathfrak{p}' \text{ et } \varphi(\mathfrak{p}_i) = \mathfrak{p}'_i$$

Tout revient à montrer que $k \leq m$.

Soit $\pi \in \mathcal{O} / \mathfrak{p} \nmid \pi$ et $\mathfrak{p}^2 \nmid \pi$. Alors $(\pi) = \mathfrak{p} \mathfrak{B}$ où $\mathfrak{p} \nmid \mathfrak{B}$

$$\bar{\mathfrak{p}} = \bar{\mathfrak{p}}' \Rightarrow \mathfrak{p}' \mid \pi$$

Soit $\omega \in \mathcal{O} / \mathfrak{B}^k \mid \omega$ et $\mathfrak{B}^k \nmid \omega$

Comme $\mathfrak{p} \nmid \mathfrak{B}^k$, on aura $\mathfrak{p} \nmid \omega$, donc $\boxed{\mathfrak{p}' \nmid \omega}$

$$\left. \begin{array}{l} \mathfrak{p}^k \mid \alpha \\ \mathfrak{B}^k \mid \omega \end{array} \right\} \Rightarrow \mathfrak{p}^k \mathfrak{B}^k \mid \alpha \omega \Leftrightarrow \pi^k \mid \alpha \omega \Rightarrow \alpha \omega = \pi^k \eta \text{ où } \eta \in \mathcal{O}$$

Comme $\mathfrak{p}' \mid \pi$, $\mathfrak{p}'^k \mid \alpha \omega$, et comme $\mathfrak{p}' \nmid \omega$, on aura $\mathfrak{p}'^k \mid \alpha$.

$$\text{d'où } \boxed{k \leq m}$$

Q.F.D.

3) Cas d'un anneau factoriel

Th : $\mathcal{D}$ est un anneau factoriel ssi il existe une théorie des diviseurs $\mathcal{D}^* \rightarrow \Delta$ ou $\mathcal{D}$ dont tous les diviseurs de Δ sont principaux.

(NB: anneau factoriel = anneau sur lequel existe une déc. unique en fact. premiers)

$(\Rightarrow)$ $\mathcal{D}$ factoriel $\Rightarrow \forall \alpha \in \mathcal{D}^* \quad \alpha = u \pi_1^{k_1} \dots \pi_m^{k_m}$ (u unité de $\mathcal{D}$)

Posons $\Delta =$ ensemble des classes d'~ de $\mathcal{D}$ pour la relation "associé à" définie par $\alpha R \beta \Leftrightarrow \exists u$ unité de $\mathcal{D} \quad \alpha = u\beta$.

Nb: on (α) la classe de $\mathcal{D}$ pour cette relation, et posons $(\alpha)(\beta) = (\alpha\beta)$.

Alors $\mathcal{D}^* \rightarrow \Delta$ définit une théorie des diviseurs sur $\mathcal{D}$.

$$\alpha \mapsto (\alpha)$$

$(\Leftarrow)$ Si tous les diviseurs de Δ sont principaux, alors :

(*) $\pi \in \mathcal{D}^*$ est premier $\Leftrightarrow (\pi)$ premier

preuve de (*) :

$(\Rightarrow)$ Si π est premier et si $(\pi) = (\alpha)(\beta)$, alors $\pi = u\alpha\beta$ où u unité de $\mathcal{D}$, donc α ou β est une unité, et (α) ou (β) sera l'unité ϵ de Δ .

$(\Leftarrow)$ Si (π) premier, soit $\pi = \alpha\beta$. Alors $(\pi) = (\alpha)(\beta)$, et donc $(\alpha) = \epsilon$ ou $(\beta) = \epsilon$, ie α ou β est une unité.

π sera donc premier.

cf p 7

$$\text{Si } \alpha \in \mathcal{D} \quad (\alpha) = (\pi_1)^{k_1} \dots (\pi_m)^{k_m} = (\pi_1^{k_1} \dots \pi_m^{k_m})$$

$$\text{entraîne } \alpha = u \pi_1^{k_1} \dots \pi_m^{k_m} \quad (\text{où } u \text{ unité de } \mathcal{D})$$

La décomposition existe bien dans $\mathcal{D}$, et est unique (facile).

cf p 7

4) Condition nécessaire d'existence d'une Théorie des diviseurs.

Th: Si $\mathcal{D}$ admet une Théorie des diviseurs, alors il est intégralement
clo (ie intégralement fermé dans son corps de fractions)

preuve:

K corps des fractions de $\mathcal{D}$.

Si $\xi \in K$ est entier sur $\mathcal{D}$, $\xi^n + a_{n-1}\xi^{n-1} + \dots + a_1\xi + a_0 = 0$ où $a_i \in \mathcal{D}$

Posez $\xi = \frac{a}{b}$

$$a^n + a_{n-1}a^{n-1}b + \dots + a_1ab^{n-1} + a_0b^n = 0 \quad (*)$$

Nb Vons $(a) = \prod_1^{k_1} \dots \prod_m^{k_m}$
 $(b) = \prod_1^{l_1} \dots \prod_m^{l_m}$

les déc. en facteurs premiers des diviseurs principaux (a) et (b) .

* Si l'on montre que $k_i \geq l_i, \forall i$, on aura l'existence de $c \in \mathcal{D} /$

$$(c) = \prod_1^{k_1-l_1} \dots \prod_m^{k_m-l_m}$$

tel que $(a) = (b)(c)$, d'où $a = ubc$, u unité de $\mathcal{D}$, et
donc $\xi = \frac{a}{b} = uc \in \mathcal{D}$.

* Notons $\prod_1 = \prod$, $k_1 = k$ et $l_1 = l$ pour simplifier.

$$\text{On a } \prod^{k(n-t)+lt} \mid a^{n-t} b^t \quad \text{pour } 1 \leq t \leq n$$

Si, par l'absurde, on avait $k < l$, alors $\prod^{k(n-1)+l}$ diviserait $a^{n-t} b^t$
pour tout $t \in \mathbb{N}_n$, et d'après (*):

$$\prod^{k(n+1)} \mid a^n$$

Comme $(a)^n = \prod_1^{k_1 n} \prod_2^{k_2 n} \dots \prod_m^{k_m n}$, c'est absurde.

absurde

CQFD

5) Lien avec les valuations

Déf: Une valuation sur le corps K est une application $v: K \rightarrow \mathbb{Z} \cup \{+\infty\}$

tel que

$$1) \quad v(0) = +\infty \quad \text{et} \quad v(K^*) = \mathbb{Z}$$

$$2) \quad v(\alpha\beta) = v(\alpha) + v(\beta)$$

$$3) \quad v(\alpha + \beta) \geq \min(v(\alpha), v(\beta))$$

* Supposons qu'il existe une théorie des diviseurs $\mathcal{D}^* \rightarrow \Delta$ sur $\mathcal{D}$.

$$\text{Alors: } \forall \alpha \in \mathcal{D}^* \quad (\alpha) = \prod_1^{\ell_1} \dots \prod_m^{\ell_m}$$

$$\text{On pose } v_{\mathfrak{p}_i}(\alpha) = \ell_i.$$

Soit K le corps des fractions de $\mathcal{D}$. Si $\xi = \frac{\alpha}{\beta} \in K^*$, on pose :

$$v_{\mathfrak{p}}(\xi) = v_{\mathfrak{p}}(\alpha) - v_{\mathfrak{p}}(\beta)$$

et l'on définit ainsi une famille $\mathcal{F}$ de valuations sur K :

$$\mathcal{F} = \{ v_{\mathfrak{p}} / \mathfrak{p} \text{ diviseur premier de } \Delta \}$$

Cette famille $\mathcal{F}$ possède des propriétés très spéciales, et l'étude de la réciproque permet d'énoncer le Théorème :

$\underline{Th}$: $\mathcal{D}$ anneau intègre

K son corps des fractions

Se donner une théorie des diviseurs sur $\mathcal{D}$ revient à se donner une famille $\mathcal{F}$ de valuations sur K telle que :

- 1) $\forall \alpha \in \mathcal{D}^* \quad v(\alpha) = 0$ presque partout
- 2) Pour $\alpha \in K$, $\alpha \in \mathcal{D} \Leftrightarrow \forall v \in \mathcal{F} \quad v(\alpha) \geq 0$
- 3) $\forall v_1, \dots, v_m \in \mathcal{F} \quad \forall k_1, \dots, k_m \in \mathbb{N} \quad \exists \alpha \in \mathcal{D} \quad v_i(\alpha) = k_i$ (*)

preuve :

($\Rightarrow$) Si $\mathcal{D}^* \rightarrow \Delta$ est une théorie des diviseurs sur $\mathcal{D}$, on considère

$$\mathcal{F} = \{ v_{\mathfrak{p}} / \mathfrak{p} \text{ premier dans } \Delta \}$$

1) est trivial

2) ($\Rightarrow$) est trivial

($\Leftarrow$) si $v_{\mathfrak{p}}(\alpha) \geq 0 \quad \forall \mathfrak{p}$, où $\alpha = \frac{a}{b} \in K$, on a :

$$\forall \mathfrak{p} \quad v_{\mathfrak{p}}(a) \geq v_{\mathfrak{p}}(b) \Rightarrow (b) | (a) \Leftrightarrow b | a \text{ dans } \mathcal{D} \\ \Rightarrow \alpha \in \mathcal{D}$$

3) Posons $\alpha = \prod_1^{k_1} \dots \prod_m^{k_m} \mathfrak{p}_i \in \Delta$

$\exists \alpha_i \in \mathcal{D}$ divisible par $\alpha_i \doteq \alpha \prod_1 \dots \prod_{i-1} \prod_{i+1} \dots \prod_m$

et non par $\prod_i^{k_i+1}$

On pose : $\alpha = \alpha_1 + \dots + \alpha_m$

On constate : $v_i(\alpha) = k_i \quad \forall i$

(*) Cette propriété d'indépendance est, en fait, générale. Elle est vérifiée par toute famille finie de valuations sur un corps K et d'ence : $\forall v_1, \dots, v_m$ valuat. sur $K \quad \forall k_1, \dots, k_m \in \mathbb{Z} \quad \exists x \in K \quad v_i(x) = k_i$ (cf Borevitch Th 3 p 202)

($\Leftarrow$) Réc., si $\mathcal{F}$ est une famille de valuations vérifiant les conditions 1) à 3) du th., on construit un monoïde Δ en définissant :

- les éléments premiers $\mathfrak{p}$ de ce monoïde : autant que de valuations dans $\mathcal{F}$.

Génèrateurs $\mathfrak{p}$ le diviseur premier associé à $v_{\mathfrak{p}} \in \mathcal{F}$

- tous les éléments de Δ : ce sont les $\mathfrak{p}_1^{k_1} \dots \mathfrak{p}_m^{k_m}$, $\mathfrak{p}_i$ premiers, $k_i \in \mathbb{N}$ tous distincts ≥ 2 .

Δ est un monoïde sur lequel la déc. en fact. premiers existe et est unique.

* 1) et 2) permettent de définir :

$$\mathcal{D}^* \longrightarrow \Delta$$

$$\alpha \longmapsto (\alpha) = \prod_{\mathfrak{p} \in \mathcal{F}} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha)}$$

qui sera un homomorphisme de monoïdes.

* Enfin, les propriétés satisfaites par $\mathcal{F}$ permettent de prouver les 3 propriétés ①②③ demandées à $\mathcal{D}^* \rightarrow \Delta$ pour définir une Théorie des diviseurs (cf §1) :

$$\textcircled{1} \text{ Si } \alpha, \beta \in \mathcal{D}^*, \alpha | \beta \text{ dans } \mathcal{D} \Leftrightarrow (\alpha) | (\beta) \text{ dans } \Delta$$

$$(\Rightarrow) \alpha | \beta \Rightarrow \exists \gamma \in \mathcal{D} \quad \beta = \alpha \gamma \Rightarrow (\beta) = (\alpha) \cdot (\gamma)$$

$$(\Leftarrow) (\alpha) | (\beta) \Rightarrow v_{\mathfrak{p}}(\alpha) \leq v_{\mathfrak{p}}(\beta) \quad \forall \mathfrak{p} \text{ premiers de } \Delta$$

$$\text{d'où } v_{\mathfrak{p}}\left(\frac{\beta}{\alpha}\right) \geq 0 \quad \forall \mathfrak{p}, \text{ d'où } \frac{\beta}{\alpha} \in \mathcal{D} \text{ d'après 2)}$$

$$\textcircled{2} \quad a \mid \alpha \text{ et } a \mid \beta \Rightarrow a \mid \alpha \pm \beta$$

$$\text{Si } a = \prod_1^{k_1} \dots \prod_m^{k_m}$$

$$a \mid \alpha \Leftrightarrow v_p(a) \leq v_p(\alpha) \quad \forall p$$

$$a \mid \beta \Leftrightarrow v_p(a) \leq v_p(\beta) \quad \forall p$$

$$a \mid \alpha \pm \beta \Leftrightarrow v_p(a) \leq v_p(\alpha \pm \beta) \quad \forall p$$

Comme $v_p(\alpha \pm \beta) \geq \min(v_p(\alpha), v_p(\beta)) \geq v_p(a)$, c'est gagné.

$$\textcircled{3} \quad a = b \Leftrightarrow \{\alpha \in \mathbb{D} / a \mid \alpha\} = \{\alpha \in \mathbb{D} / b \mid \alpha\}$$

($\Leftarrow$) Si $a \neq b$, on a par ex. $a = \prod_1^{k_1} \dots \prod_m^{k_m}$ et $b = \prod_1^{l_1} \dots \prod_m^{l_m}$ avec $k_1 > l_1$.

D'après 3), il existe $\alpha \in \mathbb{D}$ tq $v_{p_i}(\alpha) = l_i \quad \forall i$

d'où $a \nmid \alpha$ et $b \mid \alpha$. Absurde.

($\Rightarrow$) trivial.

CQFD

5)

Th : $\left. \begin{array}{l} \text{Dadmet une Théorie des} \\ \text{diviseurs avec un nbre fini} \\ \text{de diviseurs premiers} \end{array} \right\} \Rightarrow \mathcal{D} \text{ factoriel}$

preuve :

Soit la Théorie des diviseurs $\mathcal{D}^* \rightarrow \Delta$ avec $\{\mathfrak{p}_1, \dots, \mathfrak{p}_m\} = \text{diviseurs premiers de } \Delta$.

$$\forall \alpha \in \mathcal{D}^* \quad (\alpha) = \mathfrak{p}_1^{k_1} \dots \mathfrak{p}_m^{k_m}$$

D'après la condition 3) du Th du §5 :

$$\exists \pi_i \quad v_{\mathfrak{p}_j}(\pi_i) = \delta_{ij}$$

Donc $(\pi_i) = \mathfrak{p}_i$ et π_i est premier car

$$\pi_i = \alpha\beta \Rightarrow (\pi_i) = \mathfrak{p}_i = (\alpha)(\beta) \Rightarrow \mathfrak{p}_i | \alpha \text{ ou } \mathfrak{p}_i | \beta \Rightarrow \pi_i | \alpha \text{ ou } \pi_i | \beta$$

• La décomposition en facteurs premiers existe alors sur $\mathcal{D}$ car :

$$\forall \alpha \in \mathcal{D}^* \quad (\alpha) = \mathfrak{p}_1^{k_1} \dots \mathfrak{p}_m^{k_m} \Rightarrow \alpha = u \pi_1^{k_1} \dots \pi_m^{k_m}$$

où les π_i sont premiers dans $\mathcal{D}$

• Cette déc. est unique car

$$\pi_i | \alpha\beta \Rightarrow \pi_i | \alpha \text{ ou } \pi_i | \beta$$

(démontré ci-dessus)

Q.F.D

FIN

REMARQUES :

|| Pro. du 1) :

① $(\alpha) = (\beta) \Leftrightarrow \alpha \text{ et } \beta \text{ sont associés dans } \mathcal{D}$

② $(\alpha) = \epsilon \text{ élément unité de } \Delta \Leftrightarrow \alpha \text{ unité de } \mathcal{D}$

preuve :

① $(\alpha) = (\beta) \Leftrightarrow \begin{cases} (\alpha) | (\beta) \\ (\beta) | (\alpha) \end{cases} \Leftrightarrow \begin{cases} \alpha | \beta \\ \beta | \alpha \end{cases} \Leftrightarrow \alpha \text{ et } \beta \text{ associés dans } \mathcal{D}$

② Comme $\mathcal{D}^* \rightarrow \Delta$ est un morphisme de monoïdes unitaires, $(1) = \epsilon$,
et :

$(\alpha) = \epsilon \Leftrightarrow (\alpha) = (1) \Leftrightarrow \alpha \text{ et } 1 \text{ associés} \Leftrightarrow \alpha \text{ unité de } \mathcal{D}.$

Q.F.D.